Big Brother Taps the Bitstream

Declan McCullagh

Apr. 07, 1999 PT

WASHINGTON -- Bob Barr is an unlikely defender of civil liberties.

A former federal prosecutor and fierce opponent of gay rights and abortion, he recently won national notoriety as a House floor manager who argued at length for impeachment.

But on Tuesday, the staunch Georgia conservative showed up here at the Computers, Freedom, and Privacy conference to warn of the dangers of an overly intrusive government.

Barr said that as the 19th century dawned, natural resources were vital to our country. A century later, it was financial resources. Now, he said, information "will represent power in the 21st century."

"We need to look for ways to make these issues nonpartisan," Barr said, advising the audience to become active in lobbying their legislators and federal agencies.

Public outcry, he said, was what caused bank regulators to abandon the reviled "Know Your Customer" plan, as well as another scheme that would have led to a de facto national ID card. "The public was heavily involved."

Other panelists described a growing trend toward global electronic monitoring, including the latest developments in the National Security Agency's surveillance system, first documented in James Bamford's The Puzzle Palace.

Steve Wright from the UK-based Omega Foundation recounted his investigation into Echelon, an international network of highly sensitive listening posts operated in part by the supersecret NSA.

The system taps 2 million calls an hour, Wright said, and has been the subject of an investigation by the European Parliament. The report will be released in two weeks.

The Austrians have their own problems. A proposal that is nearly certain to become law will expand police surveillance capability to a level not seen since the Nazis, said Erich Moechel from Quintessenz. "They can wiretap according to this law ... without the order of an independent court," he said.

And Russia? Forget about it. The country has already banned encryption software that can be used to shield sensitive information from prying eyes. More recently, the FSB -- the successor to the KGB -- has required Internet service providers to allow agents to monitor all communications.

"[They] must maintain hardware, software, and a dedicated line to the local FSB department," Moechel said. The US government has required telephone companies to build in similar capabilities, though officials say surveillance will take place only with a court order.

A representative from the US Department of Justice said that societies had to balance freedom with security. No surveillance at all would be fine, said Scott Charney, "if everyone were law abiding, but they're not."

Charney, who heads the agency's computer crime unit, said the threats of child pornography, terrorism, and hackers like Kevin Mitnick mean technology should be restricted.

One audience member asked whether Justice Department-backed restrictions on overseas encryption sales that keep encryption out of the hands of human rights workers in Kosovo can be justified. "You have to balance a lot of competing equities," Charney replied.

The CFP conference continues through Thursday evening.

Related Wired Links:

Shaping Online Privacy
6.Apr.99

Know Your (Customer) Rights
30.Mar.99

Europe Is Listening
2.Dec.98

Spying on the Spies
27.Oct.98

Eavesdropping on Europe
30.Sep.98

Russia Ponders Net Snooping
21.Jul.98

End of story